R E P U B L I Q U E F R A N Ç A I S E

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

PCT/FR03/02536

REC'D 07 NOV 2003
WIPO PCT

BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 19 AOUT 2003

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

Martine PLANCHE

DOCUMENT DE PRIORITÉ

PRÉSENTÉ OU TRANSMIS
CONFORMÉMENT À LA
RÈGLE 17.1.a) OU b)

INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE
SIEGE
26 bis, rue de Saint Petersbourg
75800 PARIS cedex 08
Téléphone : 33 (0)1 53 04 53 04
Télécopie : 33 (0)1 53 04 45 23
www.inpi.fr

1er dépôt

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle - Livre VI

N° 11354*(

INPI
INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE
26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 33 (1) 53 04 53 04 Télécopie : 33 (1) 42 94 86 54

REQUÊTE EN DÉLIVRANCE

Cet imprimé est à remplir lisiblement à l'encre noire

DB 540 W / 0101

Réservé à l'INPI

REMISE DES PIÈCES
DATE
LIEU 16 AOUT 2002
75 INPI PARIS
N° D'ENREGISTREMENT NATIONAL ATTRIBUÉ PAR L'INPI 0210367
DATE DE DÉPÔT ATTRIBUÉE PAR L'INPI 16 AOUT 2002

Vos références pour ce dossier *(facultatif)* ~~240015 D20575 AV~~

1 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE

Cabinet REGIMBEAU
20, rue de Chazelles
75847 PARIS CEDEX 17
FRANCE

Confirmation d'un dépôt par télécopie ☐ N° attribué par l'INPI à la télécopie

2 NATURE DE LA DEMANDE — Cochez l'une des 4 cases suivantes

Demande de brevet	☒
Demande de certificat d'utilité	☐
Demande divisionnaire	☐
Demande de brevet initiale	N° Date
ou demande de certificat d'utilité initiale	N° Date
Transformation d'une demande de brevet européen *Demande de brevet initiale*	☐ N° Date

3 **TITRE DE L'INVENTION** (200 caractères ou espaces maximum)

PROCEDE ET SYSTEME DE SECURISATION DE TRANSMISSION D'INFORMATIONS SUR DES RESEAUX D TELECOMMUNICATION

4 **DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE FRANÇAISE**

Pays ou organisation
Date N°
Pays ou organisation
Date N°
Pays ou organisation
Date N°

☐ **S'il y a d'autres priorités, cochez la case et utilisez l'imprimé «Suite»**

5 **DEMANDEUR** (Cochez l'une des 2 cases) ☐ **Personne morale** ☒ **Personne physique**

Nom ou dénomination sociale		DEBLOCK
Prénoms		Alain
Forme juridique		
N° SIREN		
Code APE-NAF		
Domicile ou siège	Rue	37, rue Carnot, 78000 VERSAILLES
	Code postal et ville	
	Pays	FRANCE
Nationalité		Française
N° de téléphone *(facultatif)*		N° de télécopie *(facultatif)*
Adresse électronique *(facultatif)*		

☐ **S'il y a plus d'un demandeur, cochez la case et utilisez l'imprimé «Suite»**

1er depot

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

6 bis, rue de Saint Pétersbourg
5800 Paris Cedex 08
éléphone : 33 (1) 53 04 53 04 Télécopie : 33 (1) 42 94 86 54

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle - Livre VI

N° 11354*0

REQUÊTE EN DÉLIVRANCE

Page suite N° . 2. / .2.

R/suite

Réservé à l'INPI

REMISE DES PIÈCES
DATE
LIEU 16 AOUT 2002
75 INPI PARIS
N° D'ENREGISTREMENT
NATIONAL ATTRIBUÉ PAR L'INPI 0210367

Cet imprimé est à remplir lisiblement à l'encre noire

DB 829 W / 011001

Vos références pour ce dossier *(facultatif)*	240015 AV
4 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE FRANÇAISE	Pays ou organisation Date N°
	Pays ou organisation Date N°
	Pays ou organisation Date N°
5 DEMANDEUR (Cocher l'une des 2 cases)	☐ **Personne morale** ☒ **Personne physique**
Nom ou dénomination sociale	BEHAGHEL
Prénoms	Thibault
Forme juridique	
N° SIREN	
Code APE-NAF	
Domicile ou siège — Rue	13, rue Saint Denis, 92100 BOULOGNE
Domicile ou siège — Code postal et ville	
Domicile ou siège — Pays	~~FRANCE~~
Nationalité	~~Française~~
N° de téléphone *(facultatif)*	
N° de télécopie *(facultatif)*	
Adresse électronique *(facultatif)*	
5 MANDATAIRE (Cocher l'une des 2 cases)	☐ **Personne morale** ☒ **Personne physique**
Nom ou dénomination sociale	de CHABANNES
Prénoms	François
Forme juridique	
N° SIREN	
Code APE-NAF	
Domicile ou siège — Rue	16, rue de l'Orangerie, 78000 VERSAILLES
Domicile ou siège — Code postal et ville	
Domicile ou siège — Pays	~~FRANCE~~
Nationalité	~~Française~~
N° de téléphone *(facultatif)*	
N° de télécopie *(facultatif)*	
Adresse électronique *(facultatif)*	

10 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE (Nom et qualité du signataire)

92169

VISA DE LA PRÉFECTURE OU DE L'INPI

La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire.
Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE
26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 33 (1) 53 04 53 04 Télécopie : 33 (1) 42 94 86 54

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle - Livre VI

Cerfa N° 11354*02

REQUÊTE EN DÉLIVRANCE

Page suite N° 3. β.

BRAUN

Réservé à l'INPI

REMISE DES PIÈCES
DATE 16 AOUT 2002
LIEU 75 INPI PARIS
N° D'ENREGISTREMENT NATIONAL ATTRIBUÉ PAR L'INPI 0210367

Cet imprimé est à remplir lisiblement à l'encre noire

DB 829 W / 011001

Vos références pour ce dossier (facultatif)		
6 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE FRANÇAISE		Pays ou organisation Date N°
		Pays ou organisation Date N°
		Pays ou organisation Date N°
5 DEMANDEUR (Cochez l'une des 2 cases)		☐ Personne morale ☒ Personne physique
Nom ou dénomination sociale		JEANTEUR
Prénoms		Denis
Forme juridique		
N° SIREN		
Code APE-NAF		
Domicile ou siège	Rue	111 Avenue de Verdun
	Code postal et ville	9 2 1 3 0 Issy-les-Moulineaux
	Pays	FRANCE
Nationalité		Française
N° de téléphone (facultatif)		
N° de télécopie (facultatif)		
Adresse électronique (facultatif)		
5 DEMANDEUR (Cochez l'une des 2 cases)		☐ Personne morale ☒ Personne physique
Nom ou dénomination sociale		
Prénoms		
Forme juridique		
N° SIREN		
Code APE-NAF		
Domicile ou siège	Rue	
	Code postal et ville	
	Pays	
Nationalité		
N° de téléphone (facultatif)		
N° de télécopie (facultatif)		
Adresse électronique (facultatif)		

10 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE (Nom et qualité du signataire)

92169

VISA DE LA PRÉFECTURE OU DE L'INPI

La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire.
Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI

1er dépôt

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

REQUÊTE EN DÉLIVRANCE
page 4 / 4

BR2

Réservé à l'INPI

REMISE DES PIÈCES
DATE
LIEU 16 AOUT 2002
75 INPI PARIS
N° D'ENREGISTREMENT
NATIONAL ATTRIBUÉ PAR L'INPI 0210367

DB 540 W / 010801

Vos références pour ce dossier :
(facultatif) 240015 AV

6 MANDATAIRE (s'il y a lieu)

Nom		
Prénom		
Cabinet ou Société		Cabinet REGIMBEAU
N °de pouvoir permanent et/ou de lien contractuel		
Adresse	Rue	20, rue de Chazelles
	Code postal et ville	75847 PARIS CEDEX 17
	Pays	
N° de téléphone *(facultatif)*		01 44 29 35 00
N° de télécopie *(facultatif)*		01 44 29 35 99
Adresse électronique *(facultatif)*		info@regimbeau.fr

7 INVENTEUR (S) Les inventeurs sont nécessairement des personnes physiques

Les demandeurs et les inventeurs sont les mêmes personnes
- ☒ Oui
- ☐ Non : **Dans ce cas remplir le formulaire de Désignation d'inventeur(s)**

8 RAPPORT DE RECHERCHE Uniquement pour une demande de brevet (y compris division et transformation)

Établissement immédiat ou établissement différé
- ☒
- ☐

Paiement échelonné de la redevance *(en deux versements)*

Uniquement pour les personnes physiques effectuant elles-mêmes leur propre dépôt
- ☐ Oui
- ☐ Non

9 RÉDUCTION DU TAUX DES REDEVANCES

Uniquement pour les personnes physiques
- ☐ Requise pour la première fois pour cette invention *(joindre un avis de non-imposition)*
- ☐ Obtenue antérieurement à ce dépôt pour cette invention *(joindre une copie de la décision d'admission à l'assistance gratuite ou indiquer sa référence)* : AG ☐☐☐☐☐

Si vous avez utilisé l'imprimé «Suite», indiquez le nombre de pages jointes

10 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE
(Nom et qualité du signataire)

92169

VISA DE LA PRÉFECTURE OU DE L'INPI

La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire.
Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI.

PROCEDE ET SYSTEME DE SECURISATION DE TRANSMISSION D'INFORMATIONS SUR DES RESEAUX DE TELECOMMUNICATION.

DOMAINE TECHNIQUE GENERAL.

L'invention concerne un procédé de transmission sécurisée d'informations confidentielles, comportant éventuellement des codes d'identification, sur des réseaux de télécommunication, notamment Internet et réseau téléphonique.

Plus précisément, elle concerne un procédé évitant le transit ou le stockage des informations confidentielles, dans leur intégralité, par des intermédiaires entre un expéditeur et un destinataire des informations.

Le procédé permet en outre de construire un historique d'utilisation de l'information confidentielle, sans pour autant pouvoir la reconstituer dans son intégralité.

L'invention est particulièrement adaptée à la transmission d'un code de carte de crédit ou d'authentification dans le cadre de la sécurisation des paiements, et dans le cadre d'un accès en ligne, à caractère confidentiel notamment.

ETAT DE L'ART.

La transmission de codes confidentiels sur le réseau Internet par exemple, et particulièrement de code de carte de crédit, est essentielle pour finaliser les transactions commerciales en ligne.

Les consommateurs sont réticents à transmettre les informations confidentielles sur Internet ou sur un autre réseau de télécommunication. La réticence est un frein important au développement des transactions en ligne.

La crainte du consommateur est double :

- d'une part, il s'agit d'une peur d'un piratage de l'information vers le marchand ou même la banque, via une écoute de la ligne lors de la transmission. Le piratage peut être effectué par un tiers qui récupérerait ainsi le code confidentiel ;

- d'autre part, il s'agit également d'une peur du piratage du numéro de carte sur le serveur du marchand, ou simplement de la malhonnêteté du marchand.

Ces deux craintes se résument par la peur de transmettre le code de carte bancaire à une personne mal intentionnée.

En effet, lorsqu'une personne malhonnête s'est procurée un numéro de carte bancaire, elle peut facilement faire des achats en ligne en se faisant passer pour le propriétaire de la carte. Il est difficile de démasquer ou d'identifier le malfaiteur.

Ainsi, malgré la mise en place de système de cryptage des données lors de leur transfert, la méfiance reste de mise.

Par ailleurs, les craintes des marchands en ligne sont doubles:

- d'une part, ils craignent une répudiation excessive des achats en ligne due à la fraude, et parfois à la malhonnêteté de certains consommateurs. En pratique, pour éviter les fraudes, ils sont obligés de contracter une police d'assurance, et d'utiliser en outre des outils d'analyse de leurs fichiers de clients ;

- d'autre part, les marchands craignent aussi les attaques, sur leurs serveurs, de tiers qui veulent récupérer des numéros de cartes bancaires. Les mesures de sécurité ne sont jamais suffisantes et des milliers de numéros de cartes disponibles sur un serveur sont une cible très attractive pour des malfaiteurs.

Plusieurs procédés de sécurisation de transactions bancaires ont été proposés.

Le protocole de transaction sécurisé, ou « Secure Socket Layer (SSL) » selon la terminologie anglo-saxonne généralement utilisée par l'homme de métier, permet une bonne protection de la transmission des données.

D'autres solutions utilisent des procédés dits "propriétaires", qui imposent l'adhésion de l'acheteur et du vendeur à un système technique (par exemple lecteur de carte ou système de génération de clef propriétaire)

et/ou un processus de paiement nécessitant une préinscription plus ou moins complexe.

Enfin, la transmission des informations confidentielles par télécopie, téléphone ou courrier rassure l'utilisateur sur la transmission.

Les techniques précédentes présentent cependant des inconvénients.

Le protocole SSL présente une fragilité en terme d'authentification. En effet, transmettre un numéro de code selon ce procédé ne permet pas de limiter la fraude lorsque la carte et/ou le numéro ont été volés. Le numéro de la carte seul n'assure pas de fonction d'authentification.

Les solutions du type « propriétaire » sont très difficiles à mettre en place, car elles nécessitent une adhésion majoritaire et simultanée des usagers et des marchands. Souvent elles entraînent un surcoût supérieur à la fraude.

La transmission des informations par télécopie, téléphone ou courrier ne résout pas le problème du stockage des informations par le marchand, mal attentionné, ou vulnérable aux attaques des pirates. De plus, la transmission des informations confidentielles par télécopie, téléphone ou courrier de façon non simultanée fait perdre l'interactivité de l'achat. Par conséquent, ceci entraîne une perte d'efficacité globale, du fait qu'un certains nombres d'acheteurs s'arrêteront en cours et ne finaliseront pas leur achat.

La transmission de tous codes d'authentification autres que les codes bancaires pose des problèmes similaires de confiance et de sécurité, auxquels la transmission par deux voies séparées et deux parties complémentaires du code permet de répondre.

PRESENTATION DE L'INVENTION.

L'invention propose de pallier ces inconvénients.

Un des buts de l'invention est de permettre une plus grande authentification de l'utilisateur tout en conservant une simplicité d'usage.

Un autre but de l'invention est de fournir un procédé qui ne nécessite pas obligatoirement d'inscription préalable auprès d'un organisme de sécurisation.

Enfin un but de l'invention est de proposer un procédé de transmission d'information confidentielle évitant le stockage ou le transit de l'intégralité des informations par un organisme non autorisé.

A cet effet, l'invention propose un procédé de transmission sécurisée d'un code confidentiel d'authentification à un organisme d'authentification lors d'une transaction avec un utilisateur, caractérisé en ce que l'utilisateur transmet une première partie du code confidentiel à un fournisseur de produits ou de services sur un premier réseau, la deuxième partie complémentaire du code confidentiel étant transmise à un intermédiaire de transaction sur un autre réseau, le fournisseur et l'intermédiaire transmettant ensuite à l'organisme d'authentification la partie du code qu'ils ont reçue.

Cette séparation de l'information en deux lots qui sont transmis par des voies de communication physiquement distinctes, est facilement compréhensible par le client qui transmet une partie de son information par des moyens distincts. Il en est naturellement rassuré.

L'invention est avantageusement complétée par les caractéristiques suivantes, prises seules ou en une quelconque de leur combinaison techniquement possible :

- l'utilisateur transmet sur le deuxième réseau la deuxième partie du code confidentiel lorsqu'il est sollicité par l'intermédiaire de transaction ;
- il comporte les étapes selon lesquelles :
  - l'utilisateur valide une commande chez le fournisseur ;
  - l'utilisateur transmet sur la demande du fournisseur les informations nécessaires à son identification ou l'envoi et au paiement de la commande, notamment la première partie du code confidentiel ;
  - le fournisseur envoie à l'organisme ces informations sur un réseau sécurisé ;
  - l'utilisateur est redirigé vers l'intermédiaire de transaction ;
  - les coordonnées de rappel de l'utilisateur sont transmises à l'intermédiaire ;

- l'intermédiaire sollicite l'utilisateur en le rappelant automatiquement grâce aux coordonnées qui lui ont été transmises ;
- l'utilisateur transmet à l'intermédiaire les informations nécessaires à la validation de la commande ou de son authentification, notamment la deuxième partie du code confidentiel ;
- l'intermédiaire envoie à l'organisme la deuxième partie du code confidentiel sur un réseau sécurisé ;
- l'organisme reconstitue l'ensemble du code confidentiel, et émet un avis sur la transaction et/ou l'authentification.

- le premier réseau est du type Internet, le deuxième réseau est du type téléphonique, le réseau sécurisé entre le fournisseur, l'intermédiaire et l'organisme permettant des liaisons sécurisées point à point ;

- l'intermédiaire rappelle automatiquement l'utilisateur, ledit utilisateur étant guidé automatiquement dans les différentes étapes du procédé de transmission des informations nécessaires grâce à des moyens formant serveur ;

- la liaison entre l'utilisateur et le fournisseur est établie tout au long du procédé de validation et/ou d'authentification ;

- l'intermédiaire rappelle l'utilisateur après sa déconnexion d'avec le fournisseur, ladite liaison avec le fournisseur étant rétablie une fois que les informations nécessaires ont été transmises à l'intermédiaire ;

- les informations nécessaires sont stockées par l'intermédiaire afin que des informations sur les transactions effectuées avec ses informations stockées puissent être transmises au fournisseur lors de transactions ultérieures ;

- l'intermédiaire demande à l'utilisateur de fournir, en outre des informations nécessaires, un identifiant qui est utilisé lors des transactions ultérieures et qui permet une authentification encore plus spécifique, qui s'ajoute a celle déjà permise par l'obtention du numéro de téléphone de l'utilisateur ;

- l'identifiant est un code numérique et/ou vocal rentré sur le terminal en connexion avec le deuxième réseau ;

- le fournisseur génère lors de la validation de la transaction un identifiant de session, ledit identifiant étant transmis à l'intermédiaire et à l'organisme, afin de permettre aux différents acteurs d'échanger des informations

relatives à cette transaction, et notamment à l'organisme de reconstituer l'intégralité du code confidentiel ;

- l'intermédiaire génère lors de la validation de la transaction un identifiant de session, ledit identifiant étant transmis au fournisseur et à l'organisme, afin de permettre aux différents acteurs d'échanger des informations relatives à cette transaction, et notamment à l'organisme de reconstituer l'intégralité du code confidentiel ;

- l'organisme génère lors de la validation de la transaction un identifiant de session, ledit identifiant étant transmis au fournisseur et à l'intermédiaire, afin de permettre aux différents acteurs d'échanger des informations relatives à cette transaction, et notamment à l'organisme de reconstituer l'intégralité du code confidentiel ;

- l'intermédiaire gère et corrige l'entrée des informations nécessaires à fournir sur le deuxième réseau par l'utilisateur ;

- le code confidentiel parmi les informations complémentaires à transmettre sur les premier et deuxième réseaux comporte une partie du numéro de carte bancaire ;

- le fournisseur et l'organisme forment une seule entité ;

- l'intermédiaire et l'organisme forment une seule entité ; et

- l'intermédiaire, le fournisseur et l'organisme forment une seule entité.

L'invention concerne également un système pour la mise en œuvre du procédé selon l'invention.

PRESENTATION DES FIGURES

D'autres caractéristiques, buts et avantages de l'invention ressortiront de la description qui suit qui est purement illustrative et non limitative et qui doit être lue en regard des dessins annexés sur lesquels :

- la figure 1 représente schématiquement les échanges d'informations entre un utilisateur, un marchand, une banque et un intermédiaire de sécurisation ;

- la figure 2 représente schématiquement les différentes étapes d'un procédé de sécurisation des échanges d'informations entre un utilisateur, un marchand, une banque et un intermédiaire de sécurisation ; et

- la figure 3 représente schématiquement un enchaînement possible des différentes étapes d'un procédé de sécurisation des échanges d'informations entre un utilisateur, un marchand, une banque et un intermédiaire de sécurisation.

DESCRIPTION DETAILLEE.

La figure 1 représente schématiquement les échanges d'informations entre un utilisateur 1, un fournisseur ou marchand 2, une banque ou un organisme d'authentification 3 et un intermédiaire 4 de sécurisation lors d'une transaction quelconque en ligne sur un réseau de télécommunication.

Dans la présente description, le terme « utilisateur » fait référence à un utilisateur 1 qui veut transmettre des données quelconques, comme un internaute par exemple.

De même, les termes de « banque » ou « organisme d'authentification » font référence à l'organisme d'authentification final 3.

Le « fournisseur » ou « marchand » qualifient le fournisseur 2 de produit et service en transaction avec l'utilisateur 1.

Enfin, le terme d'« intermédiaire » de transaction désigne l'organisme 4 réalisant les étapes possibles d'un procédé selon l'invention.

La figure 1 présente un réseau de communication comportant deux parties 100 et 200.

Une troisième partie 300 du réseau de télécommunication permet une communication tripartite entre le marchand 2, la banque 3 et l'intermédiaire 4. Les doubles flèches 102, 105 et 106 symbolisent les échanges d'informations entre le marchand 2 et l'intermédiaire 4, l'intermédiaire 4 et la banque 3, et le marchand 2 et la banque 3 respectivement.

La première partie possible 100 permet une communication entre l'utilisateur 1 et le marchand 2 représentée par la double flèche 101, ainsi qu'entre l'utilisateur 1 et l'intermédiaire 4 lors d'échange 103. Elle est préférentiellement du type Internet. La première partie 100 peut donc supporter tout type de caractères devant être transmis par l'utilisateur 1.

Dans les développements qui vont suivre, on désigne par Internet tous les réseaux informatiques 100 de terminal informatique à terminal

informatique. La désignation comprend notamment toutes sortes de réseaux privés ou publics, comme intranet ou extranet par exemple.

La deuxième partie possible 200 du réseau de télécommunication permet une communication entre l'utilisateur 1 et l'intermédiaire 4 lors d'échange 104. Elle est préférentiellement du type réseau téléphonique.

Le réseau téléphonique est dans l'état de l'art actuel du parc composé de terminaux de téléphonie à touches numériques. Ainsi, les données transmises par les terminaux sont numériques dans l'état de l'art actuel. L'évolution de l'état de l'art pouvant permettre prochainement la transmission de tout type de caractères.

Ainsi, à l'extrémité du réseau 100 située près de l'utilisateur 1, le système de mise en œuvre du procédé possible selon l'invention comporte d'une part des moyens 11 de connexion au réseau 100 et d'autre part des moyens de connexion 12 au réseau 200.

Les moyens 11 communiquent avec des moyens 21 situés chez le marchand 2 et des moyens 41 situés chez le l'intermédiaire 4, afin de permettre les échanges 101 et 103 respectivement.

Les moyens 12 communiquent avec des moyens 42 situés chez l'intermédiaire 4, afin de permettre les échanges 104.

Les moyens 11 comportent par exemple un terminal informatique 11 dit « client web », puisque le réseau 100 est du type Internet.

Les moyens 12 comportent par exemple des moyens formant une connexion téléphonique fixe ou un téléphone mobile puisque le réseau 200 est du type réseau de téléphonie fixe ou mobile.

Le téléphone 12 est avantageusement à touches et permet l'envoi de codes Dual Tone Multi-Frequency (DTMF) selon la terminologie anglo-saxonne généralement utilisée.

Le procédé selon l'invention est ainsi transposable aux systèmes déjà existants, puisque les téléphones mobiles permettent l'envoi de codes DTMF et la très grande majorité des téléphones fixes sont maintenant à touches et fréquence vocale permettant l'envoi de codes DTMF.

Dans le cas où les moyens 12 de l'utilisateur 1 ne permettent pas la transmission des codes DTMF, une variante du procédé selon l'invention,

utilisant la reconnaissance vocale, est prévue. Elle est décrite en plus détails dans la suite de la description.

A l'extrémité du réseau 100 située près du marchand 2, le système comporte des moyens 21 formant serveur sur le réseau 100. Les moyens 21 comportent par exemple un serveur dit « serveur web ».

Le marchand 2 peut ainsi échanger des données 101 avec l'utilisateur 1.

La troisième partie 300 du réseau de télécommunication est préférentiellement du type apte à la transmission de données sécurisées point à point.

A titre d'exemple non limitatif, un protocole de transmission sécurisé point à point peut utiliser, par exemple, des messages signés par un MAC (Message Authentification Code) qui est un scellement calculé avec un algorithme, par exemple de type DES (Data Encryption Standard), et associé à une clé de scellement échangée avec les données.

D'autres procédés de transactions sécurisées point à point sont bien entendu connus de l'homme du métier.

Ainsi, le système chez le marchand 2 comporte également des moyens 23 aptes à gérer des transactions point à point 102 avec scellement de données.

Encore une fois, le procédé selon l'invention est transposable aux systèmes de l'art antérieur, puisque la plupart des sites marchands sont équipés de tels serveurs. Ils utilisent déjà des protocoles de transfert sécurisé de données point à point, par exemple avec échange de clef de cryptage.

Dans le cas où le marchand 2 ne possède pas les moyens 23 aptes à la gestion de telles transactions, il en confie la prestation à un tiers agréé par sa banque. Ledit tiers a mis au préalable en place avec la banque les protocoles adéquats de transfert.

Les moyens 21 et 23 du client 2 sont gérés par des moyens 22.

De la même façon, les systèmes aux extrémités du réseau 300 situées chez la banque 3 et l'intermédiaire 4 comportent des moyens 33 et 43

respectivement permettant le traitement des flux d'information en transfert sécurisé.

De plus la banque 3 possède des moyens 31 formant serveur d'authentification, ainsi que des moyens 32 permettant la gestion de l'ensemble des moyens 31 et 33.

On rappelle ici que le terme de « banque » fait référence à un organisme bancaire ou financier, mais également à un organisme 3 d'authentification quelconque.

L'intermédiaire 4 est relié aux moyens 12 sur le réseau 200 par l'intermédiaire de moyens 42 formant serveur. Les moyens 42 comportent par exemple un serveur téléphonique.

Les moyens 42 sont aptes par exemple à effectuer des appels téléphoniques 104, de faire des appels différés, de filtrer les codes DTMF, de diffuser des messages et d'enregistrer des appels. Les moyens 42 sont connus de l'homme du métier.

De plus, l'intermédiaire 4 est relié aux moyens 11 sur le réseau 100 par l'intermédiaire de moyens 41 formant serveur. Les moyens 41 comportent par exemple un serveur web.

Enfin, l'intermédiaire 4 est relié aux moyens 33 sur le réseau 300 par l'intermédiaire de moyens 43 formant serveur point à point.

L'ensemble des liaisons de mise en œuvre du procédé selon l'invention est connu de l'homme du métier.

Avantageusement, le marchand 2 et l'organisme d'authentification final 3 sont distincts.

Lors d'un achat ou d'une transaction nécessitant une authentification, l'utilisateur transmet à l'organisme 3 d'authentification final un code pour valider sa transaction avec le marchand 2.

Dans la présente description, le terme de « code » désigne tous les types de codes alphanumériques confidentiels et/ou informations liés à une authentification ou transmission secrète. Cela peut être par exemple mais non limitativement le numéro d'une carte de crédit ou un code d'authentification propre à un système de sécurité.

Préférentiellement, la partie du code transmise par téléphone est numérique. La partie du code peut elle être alphanumérique si les réseau le supporte.

Les termes « début de code » et « fin de code » ou « partie de code » désignent deux parties disjointes du code. Les parties disjointes n'ont pas de signification lorsqu'elles sont prises séparément et ne peuvent être reconstituées dans un procédé selon l'invention, puisqu'elles transitent par des chemins différents.

La taille des différentes parties est indifférente, tant que ces deux parties sont strictement complémentaires et non significatives en terme d'authentification lorsqu'elles sont prises séparément. Elles ne sont donc pas forcement de la même taille.

Avantageusement, la séparation du code en deux parties lors de sa transmission assure la sécurité de la transaction et de l'authentification. Les deux parties ne sont pas utilisables et sont sans valeur prises séparément.

Préférentiellement, on utilise, dans un mode de mise en œuvre possible du procédé, deux acteurs, à savoir le marchand 2 et l'intermédiaire 4 de transaction, pour la transmission des informations confidentielles entre l'utilisateur 1 et l'organisme 3 d'authentification final.

Le marchand 2 et l'intermédiaire 4 sont en communication avec l'utilisateur 1 selon deux modes différents, respectivement le réseau Internet 100 et le réseau téléphonique 200.

Ainsi, chacun transmet à l'organisme 3, et par le réseau 300, une des deux parties du code ou de l'information confidentielle.

Les flux d'informations échangées entre les différents acteurs sont représentés schématiquement par les doubles flèches 101, 102, 103, 104, 105 et 106.

Les flux sont décrits de façon plus détaillée sur la figure 3, laquelle reprend les numérotations similaires aux figures 1 et 2 pour des éléments identiques.

Les figures 1 et 3 représentent des modes de mise en œuvre possibles de l'invention dans lesquels les différents acteurs sont des entités différentes.

Cependant, selon des variantes, il est possible qu'une même entité puisse prendre le rôle de plusieurs acteurs, sous réserve bien entendu qu'elle en ait l'autorité. Ainsi, dans le cas de transmission de numéro de carte bancaire, seules les banques et les organismes qui sont habilités par les banques peuvent remplir plusieurs rôles, mais en aucun cas le site marchand.

C'est par exemple le cas lorsque la transaction est directement faite entre l'organisme d'authentification 3 et l'utilisateur 1. Dans ce cas, les acteurs 2, 3 sont regroupés dans une même entité.

C'est également le cas quand l'organisme d'authentification 3 est aussi l'intermédiaire de transaction 4 entre l'utilisateur 1 et le marchand 2. Les acteurs 3 et 4 sont donc regroupés.

Dans une autre variante, les acteurs 2, 3 et 4 sont regroupés dans une même entité, l'information confidentielle étant alors transmise à l'organisme 3 par deux réseaux différents.

Dans ces cas, les différents serveurs présentés comme utiles pour la réalisation du procédé peuvent fonctionner sur la même machine ou même faire partie intégrante d'un même programme. Les modes de transfert entre les différents acteurs restent les mêmes que ceux visibles aux figures 1 et 3.

Dans tous les modes de mise en œuvre du procédé selon l'invention, aucune inscription préalable n'est obligatoire.

Cependant, un suivi de l'historique de transaction est possible.

L'invention est utilisable pour des transactions de commerce électronique, et de manière plus générale, pour tout processus d'authentification et de transfert de données.

Avantageusement, le procédé comporte les étapes selon lesquelles :

- L'utilisateur 1 sépare l'information confidentielle en deux parties complémentaire et distinctes, mais inutilisables indépendamment l'une de l'autre ;

- L'utilisateur 1 transmet chacune des deux parties du code par des moyens de communication distincts, par le réseau 100 au marchand 2, et par le réseau 200 à l'intermédiaire 4. Dans la présente description, la

transmission au marchand 2 est effectuée par exemple par un réseau Internet et la transmission à l'intermédiaire 4 est effectuée par exemple par un réseau téléphonique. Avantageusement, les informations transmises sur les réseaux sont non réconciliables. On rend ainsi sans valeur le piratage et l'écoute des communications ;

- Le marchand 2 et l'intermédiaire 4 transmettent à l'organisme d'authentification 3 final la partie de code qui leur a été transmise par l'utilisateur 1.

Ainsi, selon le procédé de l'invention, seul l'organisme d'authentification 3 final récupère l'intégralité de l'information. Ni le marchand 2, ni l'intermédiaire 4 de transaction n'ont accès à l'intégralité de l'information.

Les deux parties de l'information, une fois réunies par l'organisme d'authentification 3, ne transitent plus que sur des réseaux sécurisés réputés non accessibles.

De fait, aucun intermédiaire n'a connaissance de l'ensemble de l'information confidentielle, et aucun ne peut stocker l'intégralité du code confidentiel.

L'invention concerne également l'utilisation qui peut être faite du couple formé par le numéro de téléphone reçu d'un utilisateur et une partie non signifiante du code d'authentification.

Ce couple permet de construire au niveau de l'intermédiaire 4 un historique des transactions pouvant être utilisé, non seulement à des fins de reporting, mais aussi par exemple à des fins de qualification du risque potentiel client, en fonction du bon règlement ou non de la transaction lors des tentatives antérieures.

Lors de chaque transaction, l'intermédiaire 4 de transaction stocke dans une base de données, par exemple comprise dans les moyens 44, le numéro de téléphone et la partie non signifiante du code d'authentification qu'il a reçus.

Les données sont soit stockées en clair, soit uniquement stockées sous une forme d'empreinte numérique, par exemple en utilisant un

mécanisme de type MD5 (« Message Digest 5 » en terminologie anglo-saxonne) connu en soi de l'homme du métier.

L'historique ainsi créé pourra être fourni au marchand lorsqu'un utilisateur 1 viendra se connecter au site du marchand 2 en fournissant le numéro de téléphone stocké et/ou la partie non signifiante. Ainsi, l'intermédiaire 4 peut indiquer au marchand 2 s'il est associé à ce couple ou à une partie de ce couple des problèmes de paiement par exemple.

De même, il est possible d'indiquer au marchand 2 si c'est la première fois qu'un tel couple est rentré lors de la transaction, ou qu'un élément du couple a changé, etc.

On indique ainsi au marchand les transactions qui représentent un plus grand danger pour le marchand 2.

En tout état de cause, le fait de devoir fournir dans un mode de réalisation préféré un numéro de téléphone, qui a une traçabilité relativement importante, permet de décourager une certaine catégorie de clients malhonnêtes.

De même, on peut bloquer par exemple les numéros de cabine téléphoniques publiques, afin d'être sûr de fournir au marchand 2 un numéro de téléphone qui renvoie à un domicile ou personne bien identifié.

Il est ainsi possible de sécuriser les transactions, et de réduire les prix des polices d'assurance qu'est souvent amené à contracter le marchand 2 dans la situation de l'art antérieur.

Toutes sortes d'autres informations peuvent être associées à ce couple permettant de former un historique des transactions effectuées par l'utilisateur 1, comme par exemple un identifiant de marchand, un montant, etc.

On va maintenant décrire plus en détail les différentes étapes du procédé selon l'invention. Les exemples suivants sont la à titre d'exemple et ne sont pas limitatifs. Par exemple, il s'agit dans cette exemple de règlement d'achat par une transaction par carte bancaire, mais il pourrait également s'agir d'une authentification quelconque, sans forcément achat. Ainsi le code à transmettre n'est pas forcément le numéro d'une carte bancaire.

La figure 2 présente un mode de mise en œuvre d'une transaction sur un réseau du type Internet.

La figure 3 reprend schématiquement, et avec les mêmes références numériques, les flux d'informations s'échangeant entre les différents acteurs lors de la mise en œuvre du procédé selon les étapes de la figure 2.

A l'étape 201 de la figure 2, après avoir par exemple sélectionné des articles dans le catalogue d'un marchand 2, l'internaute 1 décide de valider son panier d'articles.

En 202, au cours du processus de validation de la commande, le marchand 2 demande à l'internaute 1 de lui transmettre les informations nécessaires à l'envoi et au paiement des produits de la commande.

Parmi ces informations, le marchand 2 ne demande que par exemple les huit premiers chiffres du numéro de carte bancaire de l'internaute 1. La transaction s'effectue de préférence en mode sécurisé SSL.

En 203, l'internaute 1 envoie les informations demandées au marchand 2.

Lors de l'étape 204, le marchand 2 génère un identifiant de session. C'est un identifiant propre à la transaction. Il va permettre aux différents acteurs d'échanger des informations relatives à cette transaction. Cet identifiant peut selon une variante être généré plus en amont dans la transaction, soit être fourni par l'intermédiaire 4, soit être fourni par la banque 3 en réponse à la demande du marchand 2, lors des étapes 205 ou 207 détaillées plus bas dans la description.

A ce stade, le marchand 2 peut stocker les informations en attente de paiement dans une base de données, par exemple comprise dans les moyens 22, avec pour clé cet identifiant de session par exemple.

Lors de l'étape 205, le marchand 2 envoie à la banque 3 la première partie du numéro de carte bancaire accompagné de l'identifiant de session, ainsi que les autres données nécessaires pour finaliser la transaction avec la banque 3. Les autres informations nécessaires sont par exemple la date d'expiration de validité de la carte bleue, le montant de la transaction, le nom du porteur 1 de la carte, etc.

Les données nécessaires à la banque 3 sont transmises en mode sécurisé point à point comme représenté à la figure 1.

En 206, la banque 3 stocke les données transmises par le marchand 2 en attendant les informations complémentaires en provenance de l'intermédiaire de transaction 4 ayant pour clé par exemple l'identifiant de session et l'identifiant du marchand 2.

Simultanément aux étapes 205, 206, se déroule l'étape 207 selon laquelle l'internaute 1 est redirigé vers le site de l'intermédiaire 4 de transaction sur le réseau de télécommunication. L'identifiant de session est alors transmis à l'intermédiaire 4.

Selon une variante, si le marchand 2 possède déjà le numéro de téléphone de son client 1, ou s'il veut transmettre à l'intermédiaire 4 d'autres informations sur la transaction, il peut les lui transmettre en parallèle via une liaison sécurisée point à point.

Dans l'étape 208, si aucun numéro de téléphone ne lui a été transmis, l'intermédiaire 4 de transaction demande à l'internaute 1 un numéro auquel ce dernier peut être contacté immédiatement. Il s'agit alors d'un numéro de téléphone fixe ou téléphone mobile.

Si nécessaire et pour des raisons de confort et d'interactivité, le numéro de téléphone peut être demandé, s'il ne l'a pas été fait au préalable, à l'internaute 1 lors de l'étape 202 et transmis par l'internaute 1 en étape 203. Dans ce cas, lors de l'étape 207, le numéro est transmis à l'intermédiaire 4 de transaction.

A l'étape 209, l'intermédiaire 4 gère tout ce qui concerne l'appel téléphonique et ceci comprend notamment détection du mauvais format du numéro ou des numéros listés comme à risque. Il s'agit notamment des cabines téléphoniques par exemple, ou numéro utilisé lors de précédentes tentatives frauduleuses. L'intermédiaire 4 gère également la détection d'occupation de ligne, la détection de faux numéros...

Des réponses appropriées à chaque cas sont apportées.

Dans ce cas, une correction du numéro de téléphone par l'utilisateur 1 est demandée. Il est possible ainsi de fournir un rappel en différé et/ou en mode vocal, ou une annulation de la transaction.

L'intermédiaire 4 vérifie aussi si l'internaute 1 utilise ce téléphone comme accès sur le réseau Internet 100. Dans ce cas, il est demandé à l'internaute 1 de terminer sa connexion Internet. Il est alors rappelé automatiquement, par exemple cinq minutes plus tard, et guidé dans les étapes 210 à 212 en mode vocal par exemple.

L'étape de fin de guidage vocal se termine alors par l'envoi d'un courrier électronique, avec une adresse - ou URL (Uniform Resource Locator) selon la terminologie anglo-saxonne – incluse, qui lui permet de poursuivre sa transaction une fois que l'utilisateur 1 est reconnecté. Selon des variantes possibles, cet email peut être envoyé à l'issue des étapes 213 à 220.

Selon une variante possible, si le code de l'utilisateur n'est pas validé par l'organisme 3, alors l'intermédiaire 4 rappelle l'internaute 1.

A l'étape 210, l'internaute 1 reçoit un appel téléphonique de la part de l'intermédiaire 4. Il est guidé sur son client téléphonique et/ou sur son client web.

A l'étape 211, l'internaute 1 entre sur son terminal 12, dans notre exemple le téléphone, les chiffres complémentaires des chiffres entrés sur le réseau 100, dans notre exemple les huit derniers chiffres de son numéro de carte.

Il valide l'entrée des numéros sur son terminal 12, par exemple en appuyant sur la touche '#'.

Si le téléphone 12 de l'internaute 1 n'est pas à fréquence vocale, alors il peut entrer les numéros via un système de reconnaissance vocale.

Lors de l'étape 212, l'intermédiaire 4 vérifie qu'il a bien reçu les chiffres complémentaires, à savoir dans notre cas huit chiffres, puis la connexion téléphonique sur le réseau 200 est terminée. Il invite éventuellement l'utilisateur 1 à corriger les erreurs, par exemple de saisie de numéro.

En variante, lors de la première transaction avec l'intermédiaire 4, l'utilisateur 1 entre un code additionnel dit code personnel, soit en reprenant un code qui lui serait fournis par ailleurs, soit en composant un code de son choix.

En variante également, le code personnel est remplacé par une signature vocale. L'utilisateur 1 en fin de transaction est amené à prononcer son nom. Cette signature vocale est stockée et pourra être utilisée en cas de litige.

Selon encore une variante, le code est remplacé par une empreinte vocale au choix de l'utilisateur ou prédéfinie. L'empreinte qui est utilisée est reconnue par un système de reconnaissance vocale lors des utilisations suivantes de ce couple numéro de téléphone/code confidentiel, afin d'authentifier la transaction.

Lors des utilisations suivantes de ce couple numéro de téléphone/code confidentiel, le code personnel sera redemandé.

A l'étape 213, les huit derniers chiffres reçus et l'identifiant de session sont transmis en mode sécurisé point à point à la banque 3.

Lors de l'étape 214, la banque 3 reçoit les données. Avec l'identifiant de session, elle retrouve les informations d'authentification, dont les huit premiers chiffres.

Lors de l'étape 215, le numéro de carte bancaire complet est reconstitué par la banque 3.

A l'étape 216, la banque 3 valide ou ne valide pas la transaction et génère une réponse.

En 217, la réponse en transmise parallèlement par des transmissions sécurisées point à point vers l'intermédiaire 4 de transaction et vers le marchand 3.

Ensuite, lors de l'étape 218, l'intermédiaire 4 de transaction envoie le numéro de téléphone ayant servi à la transaction au marchand 2, via une transmission sécurisée point à point. C'est un numéro de téléphone valide et bien lié à l'internaute, qui constitue ainsi une trace de l'internaute 1.

En 219, l'intermédiaire 4 termine le dialogue avec l'internaute 1. Il le redirige vers le marchand 2 en passant l'identifiant de session en paramètre.

Enfin en 220, le marchand 2 termine la transaction avec l'internaute 1, par exemple en confirmant la transaction.

Comme indiqué plus haut dans la description, selon une variante préférée, l'intermédiaire 4 peut stocker des informations concernant les transactions, comme le numéro de téléphone ou la fin du code par exemple. Les informations stockées lui permettent de construire un historique des transactions.

De plus l'intermédiaire 4 peut également transmettre en temps réel au fournisseur 2 une note ou un message concernant l'historique des transactions utilisant ce couple numéro de téléphone et/ou fin du code. Les informations ainsi transmises permettent au fournisseur 2 de décider en temps réel de terminer ou de ne pas terminer la transaction. Les transactions sont ainsi sécurisées pour le marchand 2.

Ainsi, le procédé selon l'invention possède de nombreux avantages, dont notamment le fait d'utiliser des voies de transmission classiques et facilement accessibles telles que

- des transmissions sur le réseau Internet 100 ouvert, dont l'accès est relativement aisé. Ces transmissions peuvent être sécurisées ou non sécurisées par des cryptages.
- des transmissions dites spécialisées entre deux sites certifiés qui peuvent transiter, soit via le réseau Internet avec des procédés de scellement de données, soit sur d'autres réseaux garantissant une confidentialité point à point 300. Ces transmissions sont privatives entre des professionnels reconnus (les banques, leurs prestataires agréés).
- enfin des liaisons aboutissant sur le réseau téléphonique 200.

Seul le destinataire final autorisé a accès à l'ensemble des informations confidentielles.

Avantageusement, l'intermédiaire 4 peut appeler des utilisateurs 1 dans le monde entier, et/ou recevoir des appels téléphoniques venant du monde entier. Dans ce cas, avantageusement, la grandeur du réseau 200 est transparente pour chaque utilisateur 1, notamment au niveau coût de connexion ou d'appel. Le réseau 200 s'adapte ainsi au réseau 100 qui est souvent à l'échelle mondiale, pour Internet notamment.

Toutes les étapes du procédé sont automatisées sans intervention humaine. Le procédé est ainsi interactif.

Dans une mise en œuvre préférée, tout au long du déroulement du procédé, l'utilisateur 1 reste en contact simultané avec la session du site Internet du marchand 2, la session du site de l'intermédiaire 4 de transaction, et la liaison téléphonique 200 avec le serveur de l'intermédiaire 4 de transaction.

Cette interactivité permet de conserver l'utilisateur et d'éviter qu'il n'abandonne avant l'étape finale de sa transaction.

Les transactions sont hautement sécurisées par le système du rappel par l'intermédiaire 4 de l'utilisateur 1.

L'utilisateur méfiant peut mémoriser numéro de téléphone qui l'a rappelé s'il a un affichage des appels entrants ou l'obtenir par prestation de service des opérateurs de téléphonie.

REVENDICATIONS.

1. Procédé de transmission sécurisée d'un code confidentiel d'authentification à un organisme (3) d'authentification lors d'une transaction avec un utilisateur (1), caractérisé en ce que l'utilisateur transmet une première partie du code confidentiel à un fournisseur (2) de produits ou de services sur un premier réseau (100), la deuxième partie complémentaire du code confidentiel étant transmise à un intermédiaire de transaction (4) sur un autre réseau (200), le fournisseur (2) et l'intermédiaire (4) transmettant ensuite à l'organisme d'authentification (3) la partie du code qu'ils ont reçue.

2. Procédé selon la revendication 1, caractérisé en ce que l'utilisateur (1) transmet sur le deuxième réseau (200) la deuxième partie du code confidentiel lorsqu'il est sollicité par l'intermédiaire (4) de transaction.

3. Procédé selon l'une des revendications 1 ou 2, caractérisé en ce qu'il comporte les étapes selon lesquelles :

- l'utilisateur (1) valide une commande chez le fournisseur (2) ;
- l'utilisateur (1) transmet sur la demande du fournisseur (2) les informations nécessaires à son identification ou l'envoi et au paiement de la commande, notamment la première partie du code confidentiel ;
- le fournisseur (2) envoie à l'organisme (3) ces informations sur un réseau sécurisé ;
- l'utilisateur (1) est redirigé vers l'intermédiaire (4) de transaction ;
- les coordonnées de rappel de l'utilisateur (1) sont transmises à l'intermédiaire (4) ;
- l'intermédiaire (4) sollicite l'utilisateur (1) en le rappelant automatiquement grâce aux coordonnées qui lui ont été transmises ;
- l'utilisateur transmet à l'intermédiaire les informations nécessaires à la validation de la commande ou de son authentification, notamment la deuxième partie du code confidentiel ;

- l'intermédiaire (4) envoie à l'organisme (3) la deuxième partie du code confidentiel sur un réseau sécurisé ;
- l'organisme (3) reconstitue l'ensemble du code confidentiel, et émet un avis sur la transaction et/ou l'authentification.

4. Procédé selon l'une des revendications 1 à 3, caractérisé en ce que le premier réseau (100) est du type Internet, le deuxième réseau (200) est du type téléphonique, le réseau sécurisé (300) entre le fournisseur (2), l'intermédiaire (4) et l'organisme (3) permettant des liaisons sécurisées point à point.

5. Procédé selon l'une des revendications 1 à 4, caractérisé en ce que l'intermédiaire (4) rappelle automatiquement l'utilisateur (1), ledit utilisateur étant guidé automatiquement dans les différentes étapes du procédé de transmission des informations nécessaires grâce à des moyens (41, 42) formant serveur.

6. Procédé selon l'une des revendications 1 à 5, caractérisé en ce que la liaison entre l'utilisateur (1) et le fournisseur (2) est établie tout au long du procédé de validation et/ou d'authentification.

7. Procédé selon l'une des revendications 1 à 5, caractérisé en ce que l'intermédiaire (4) rappelle l'utilisateur (1) après sa déconnexion d'avec le fournisseur (2), ladite liaison avec le fournisseur (2) étant rétablie une fois que les informations nécessaires ont été transmises à l'intermédiaire (4).

8. Procédé selon l'une des revendications 1 à 7, caractérisé en ce que les informations nécessaires sont stockées par l'intermédiaire (4) afin que des informations sur les transactions effectuées avec ses informations stockées puissent être transmises au fournisseur (2) lors de transactions ultérieures.

9. Procédé selon l'une des revendications 1 à 8, caractérisé en ce que l'intermédiaire demande à l'utilisateur de fournir, en outre des informations nécessaires, un identifiant qui est utilisé lors des transactions ultérieures et qui permet une authentification encore plus spécifique, qui s'ajoute a celle déjà permise par l'obtention du numéro de téléphone de l'utilisateur.

10. Procédé selon la revendication 9, caractérisé en ce que l'identifiant est un code numérique et/ou vocal rentré sur le terminal (12) en connexion avec le deuxième réseau (200).

11. Procédé selon l'une des revendications 3 à 10, caractérisé en ce que le fournisseur (2) génère lors de la validation de la transaction un identifiant de session, ledit identifiant étant transmis à l'intermédiaire (4) et à l'organisme (3), afin de permettre aux différents acteurs d'échanger des informations relatives à cette transaction, et notamment à l'organisme (3) de reconstituer l'intégralité du code confidentiel.

12. Procédé selon l'une des revendications 3 à 10, caractérisé en ce que l'intermédiaire (4) génère lors de la validation de la transaction un identifiant de session, ledit identifiant étant transmis au fournisseur (2) et à l'organisme (3), afin de permettre aux différents acteurs d'échanger des informations relatives à cette transaction, et notamment à l'organisme (3) de reconstituer l'intégralité du code confidentiel.

13. Procédé selon l'une des revendications 3 à 10, caractérisé en ce que l'organisme (3) génère lors de la validation de la transaction un identifiant de session, ledit identifiant étant transmis au fournisseur (2) et à l'intermédiaire (4), afin de permettre aux différents acteurs d'échanger des informations relatives à cette transaction, et notamment à l'organisme (3) de reconstituer l'intégralité du code confidentiel.

14. Procédé selon l'une des revendications 3 à 13, caractérisé en ce que l'intermédiaire (4) gère et corrige l'entrée des informations nécessaires à fournir sur le deuxième réseau par l'utilisateur (1).

15. Procédé selon l'une des revendications 1 à 14, caractérisé en ce que le code confidentiel parmi les informations complémentaires à transmettre sur les premier (100) et deuxième (200) réseaux comporte une partie du numéro de carte bancaire.

16. Procédé selon l'une des revendications 1 à 15, caractérisé en ce que le fournisseur (2) et l'organisme (3) forment une seule entité.

17. Procédé selon l'une des revendications 1 à 16, caractérisé en ce que l'intermédiaire (4) et l'organisme (3) forment une seule entité.

18. Procédé selon l'une des revendications 1 à 17, caractérisé en ce que l'intermédiaire (4), le fournisseur et l'organisme (3) forment une seule entité.

19. Système de transmission sécurisée d'un code confidentiel d'authentification lors d'une transaction comportant un utilisateur (1) en transaction avec un fournisseur (2) de produits ou de services, un organisme (3) d'authentification et un intermédiaire de transaction (4) caractérisé en ce que l'utilisateur (1) comporte des moyens (11) aptes à transmettre une première partie du code confidentiel à des moyens (21) compris dans le fournisseur (2) sur un premier réseau (100), l'utilisateur comportant en outre des moyens (12) aptes à transmettre la deuxième partie complémentaire du code confidentiel à des moyens (42) compris dans l'intermédiaire de transaction (4) sur un autre réseau (200), le fournisseur (2) et l'intermédiaire (4) comportant en outre des moyens aptes à transmettre ensuite des moyens (33, 31) compris dans l'organisme d'authentification (3) la partie du code qu'ils ont reçue.

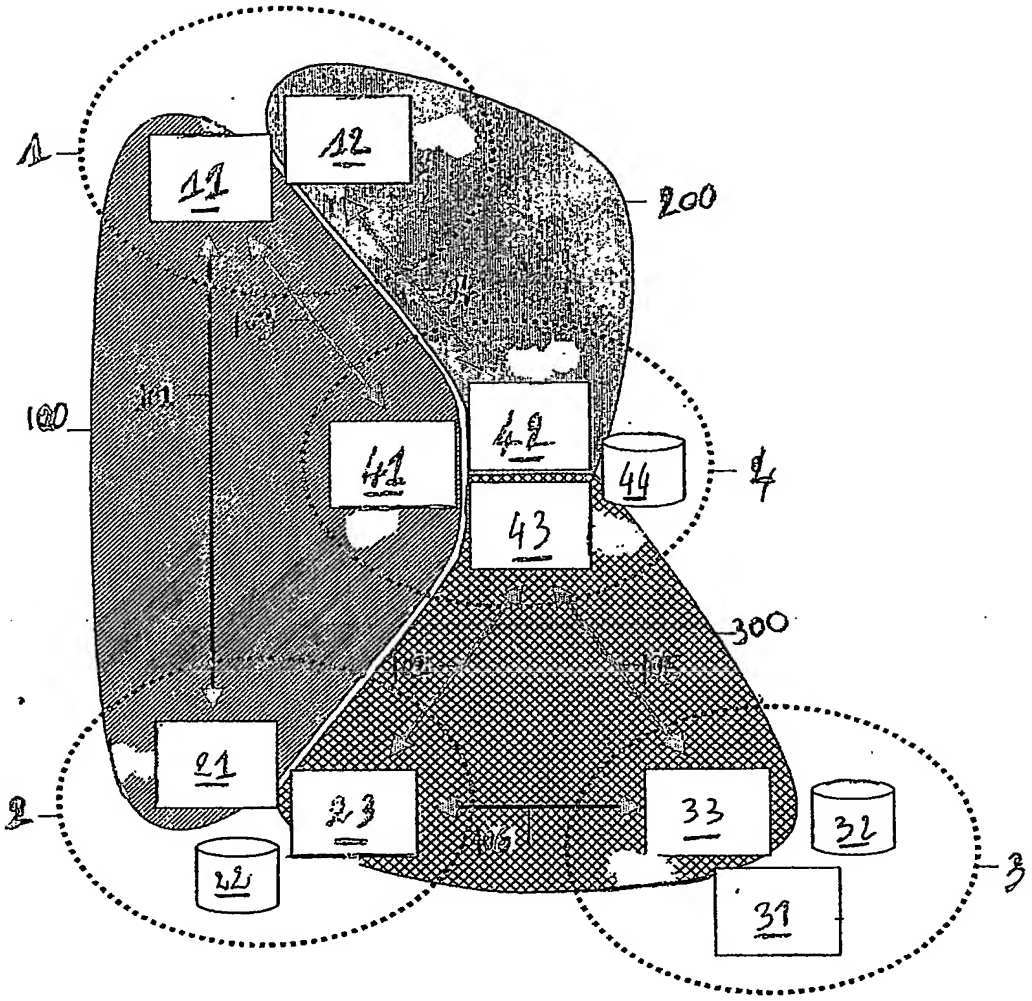
20.Système selon la revendication 19, caractérisé en ce que l'intermédiaire (4) comporte des moyens (42, 44) aptes à rappeler automatiquement l'utilisateur (1) sur le deuxième réseau (200) afin que l'utilisateur transmette la deuxième partie du code confidentiel.

21.Système selon l'une des revendications 19 ou 20, caractérisé en ce que l'intermédiaire comporte des moyens (44) aptes à gérer automatiquement et corriger l'entrée des informations nécessaires par l'utilisateur et/ou des informations complémentaires pour la sécurisation de la transaction.

22. Système selon l'une des revendications 19 à 21, caractérisé en ce que l'intermédiaire (4) comporte des moyens (44) aptes à stocker les informations complémentaires fournies par l'utilisateur.

23.Système selon l'une des revendications 19 à 22, caractérisé en ce que le fournisseur (2), l'organisme (3) et l'intermédiaire (4) comportent des moyens aptes à gérer un identifiant de session leur permettant d'échanger et/ou retrouver des informations sur la transaction.

Figure 1



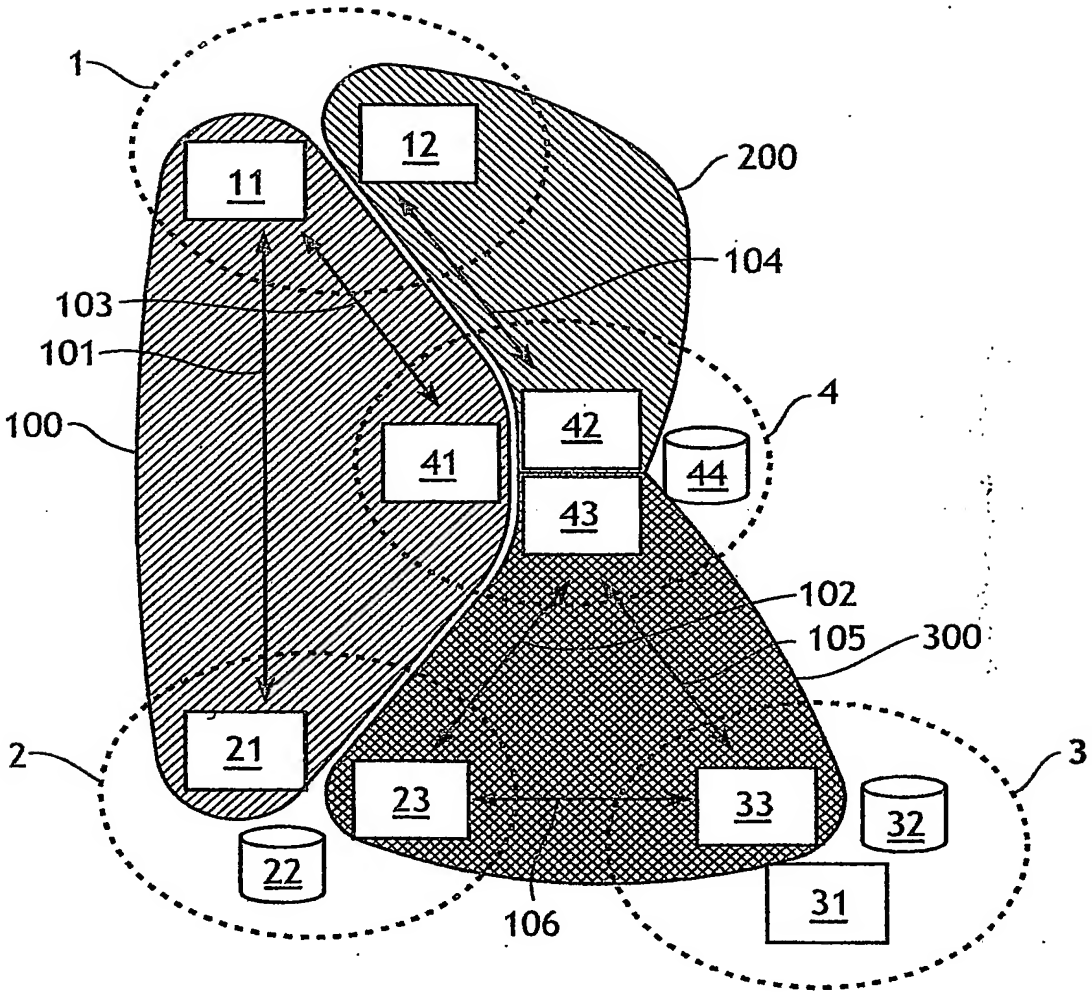
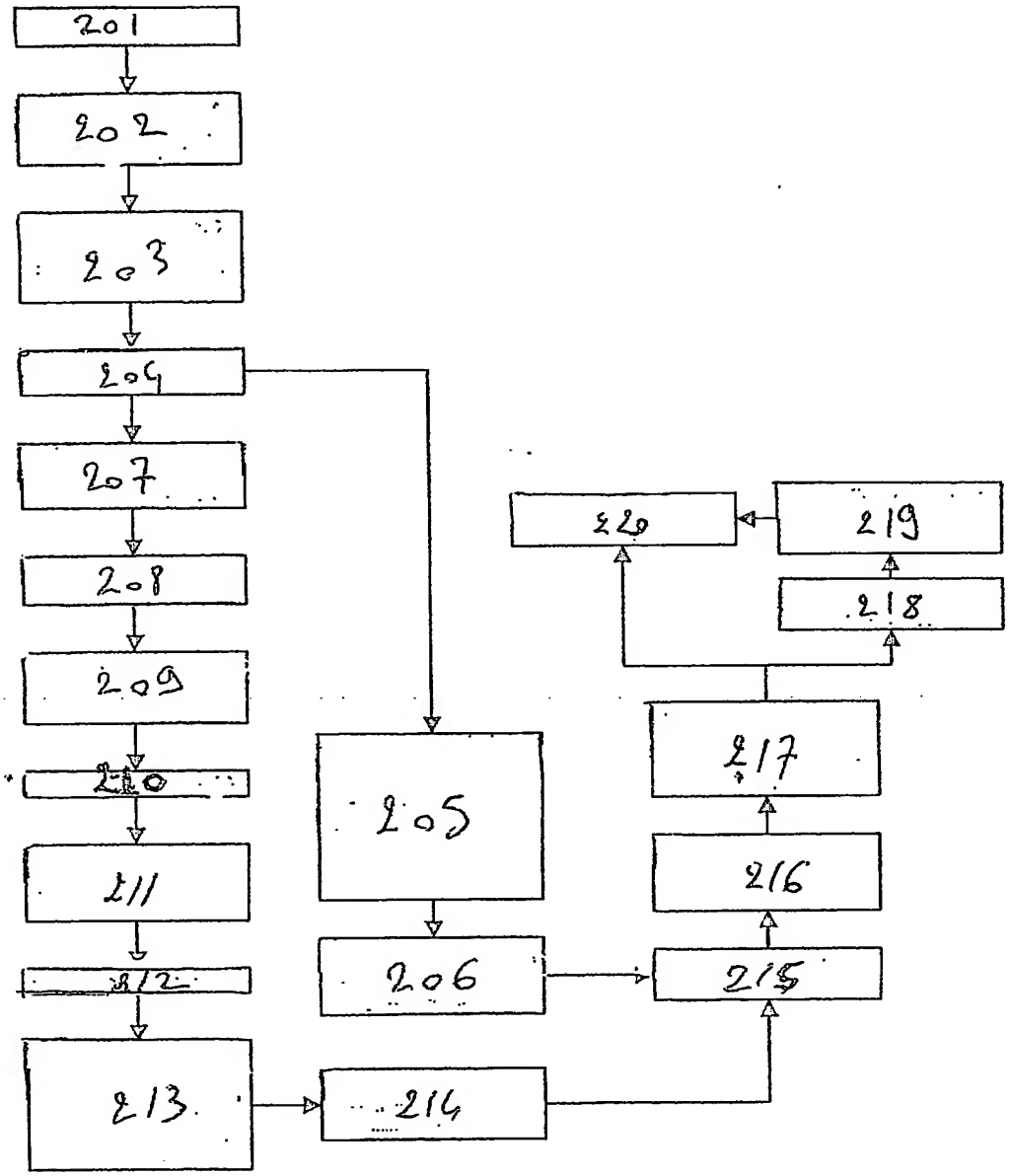

1
12
11
200
104
103
101
4
100
42
41
44
43
102
105
300
2
21
3
23
33
32
22
31
106

FIG.I

Figure 2



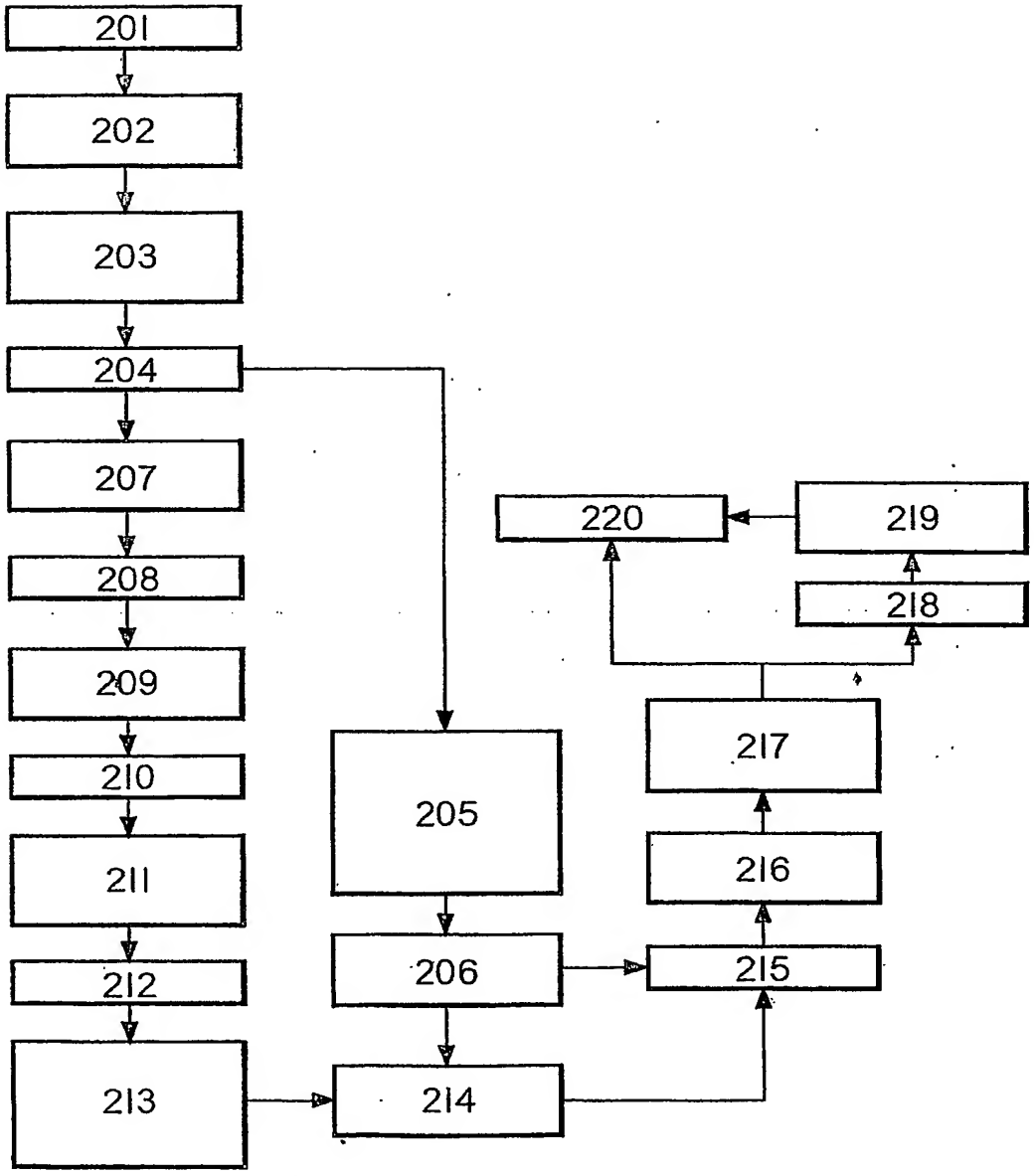
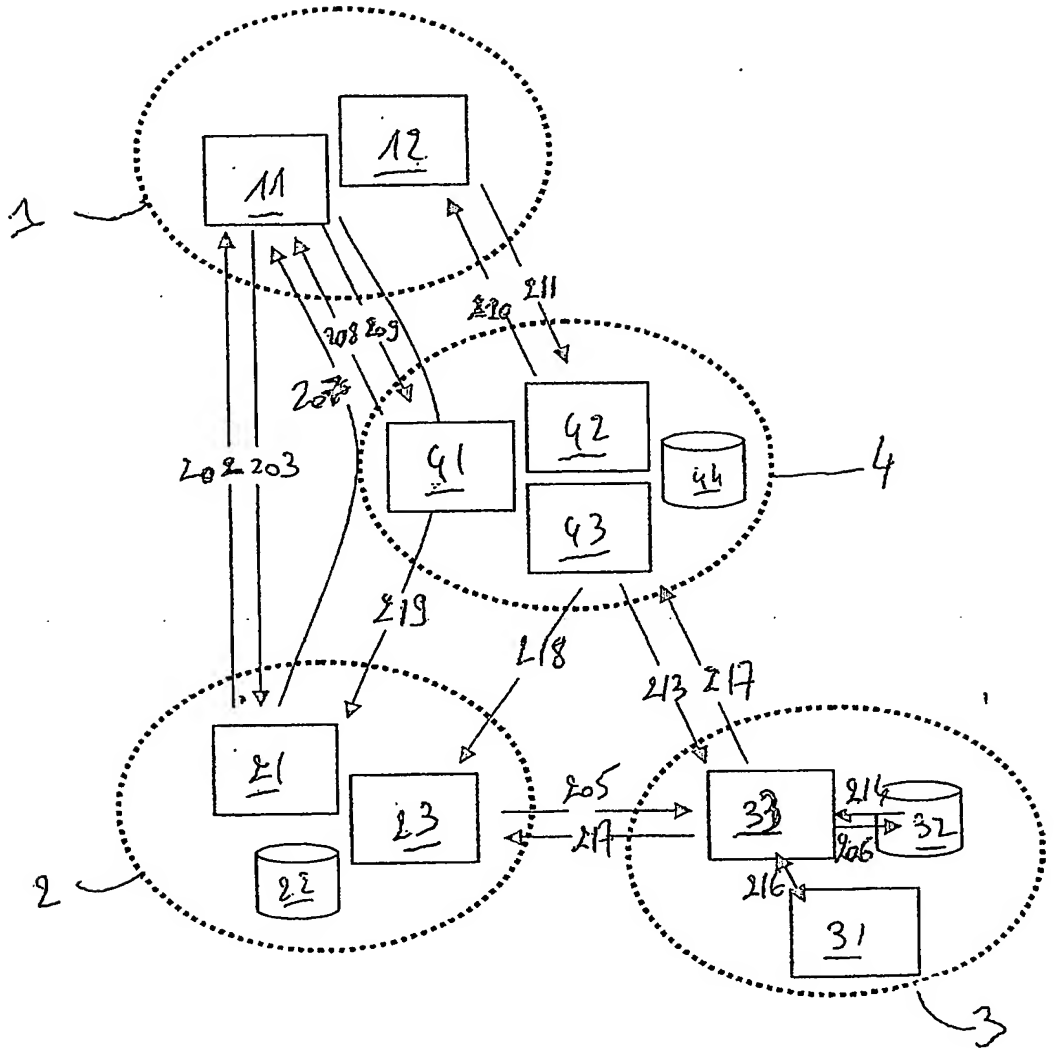

201
202
203
204
207
208
209
210
211
212
213
205
206
214
215
216
217
218
219
220

FIG.2

Figure 3



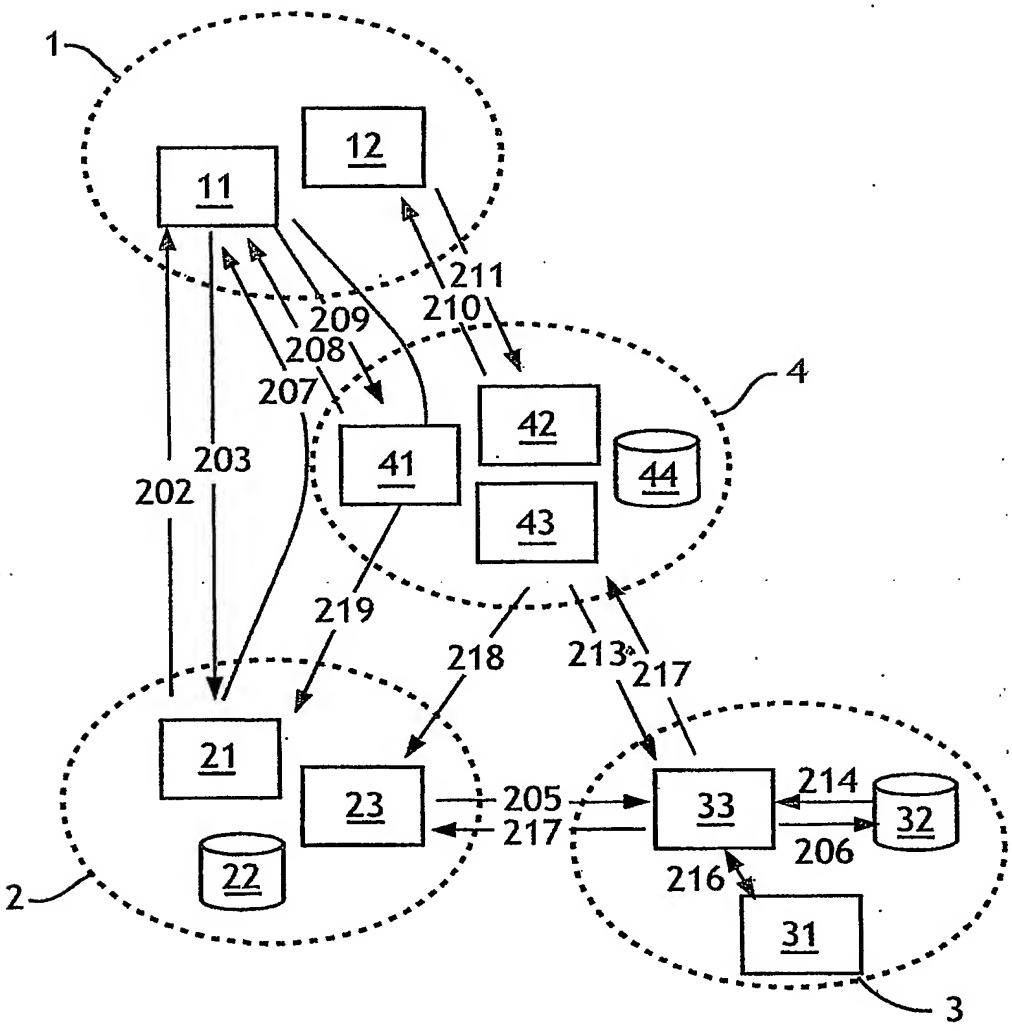

1
11
12
211
210
209
208
207
4
42
41
44
43
202
203
219
218
213
217
21
23
205
217
33
214
32
206
216
22
2
31
3

FIG.3